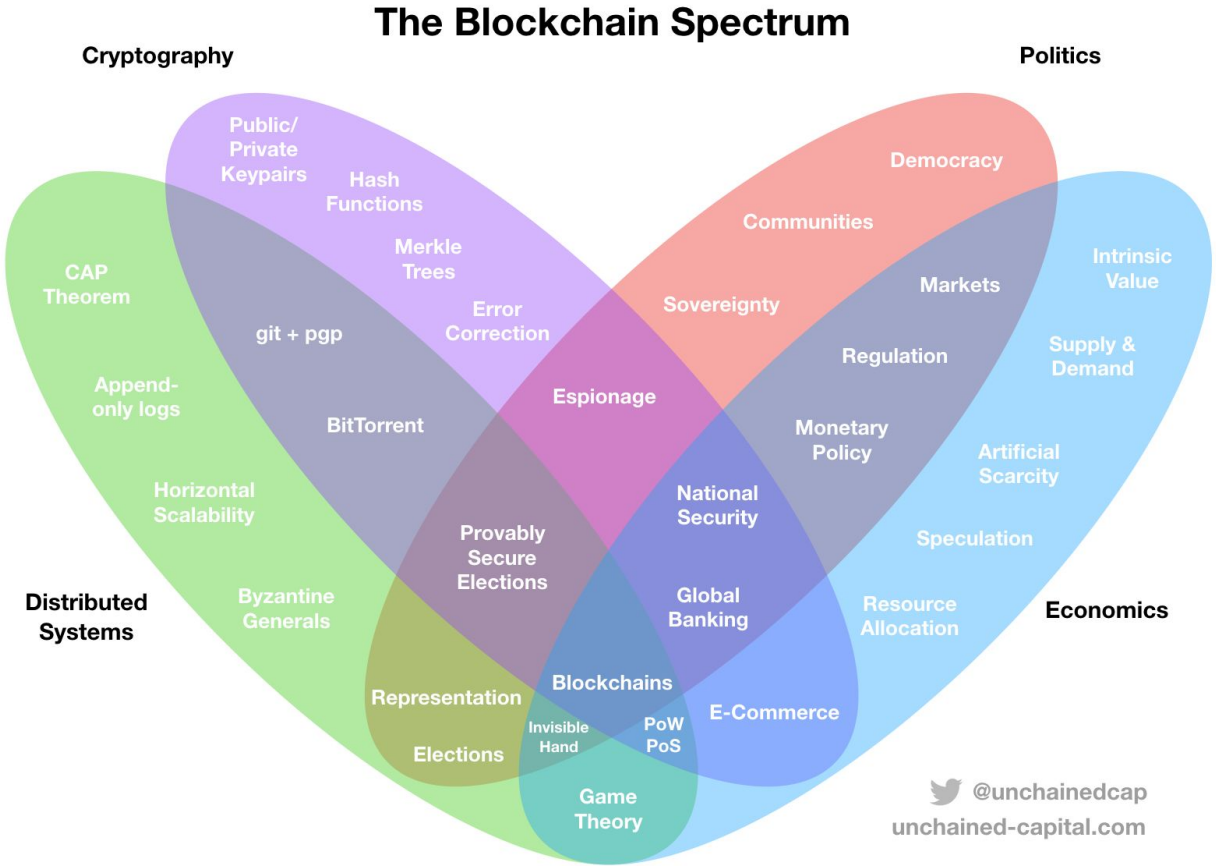
I’m A Blockchain Engineer, Ask me Anything

Destry Saul
AAS Winter Meeting
Jan 7, 2019



unchained capital

My Work History

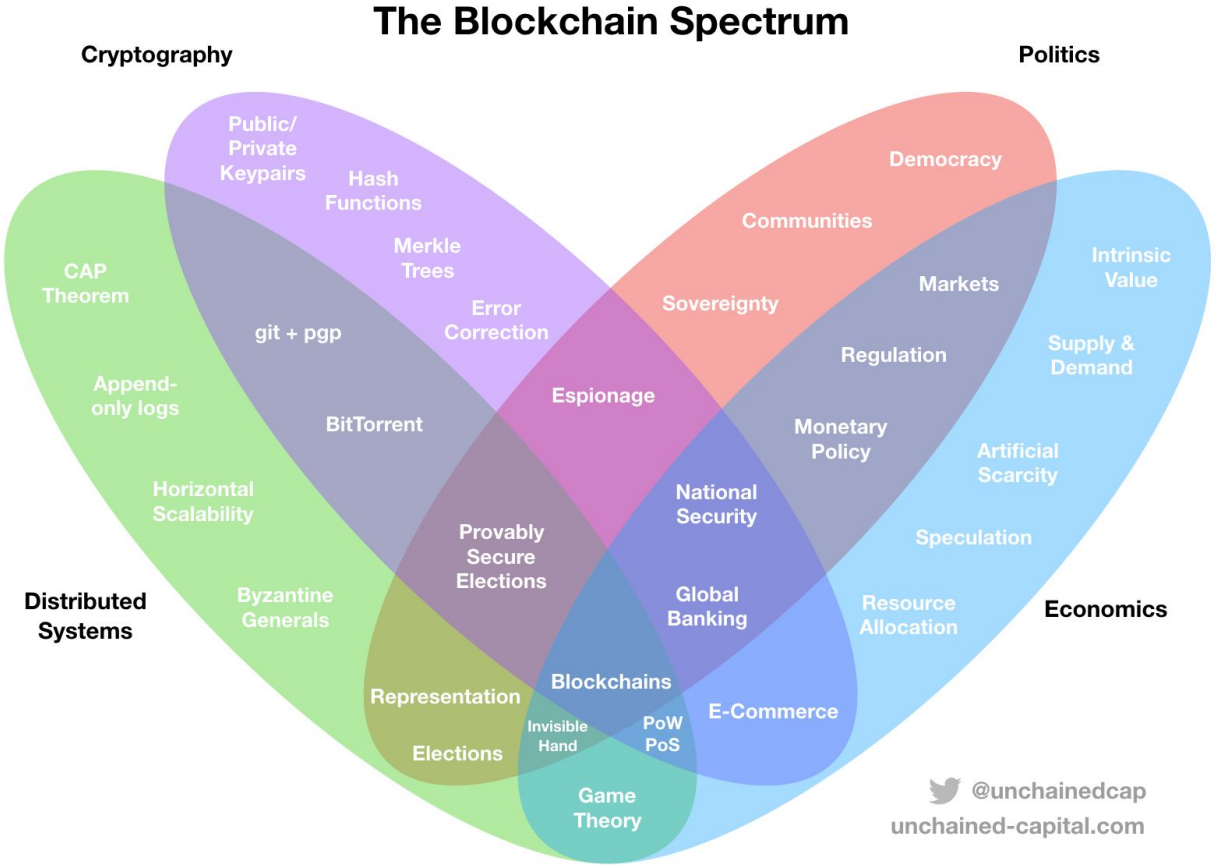
Thesis: Radio Observations - Galactic HI with Arecibo

Big Data Engineering/Architecture & Sales Engineering
Mostly fighting with Amazon
Great team, and accommodating

Data Scientist! - mostly fighting for access to data

Blockchain Engineer

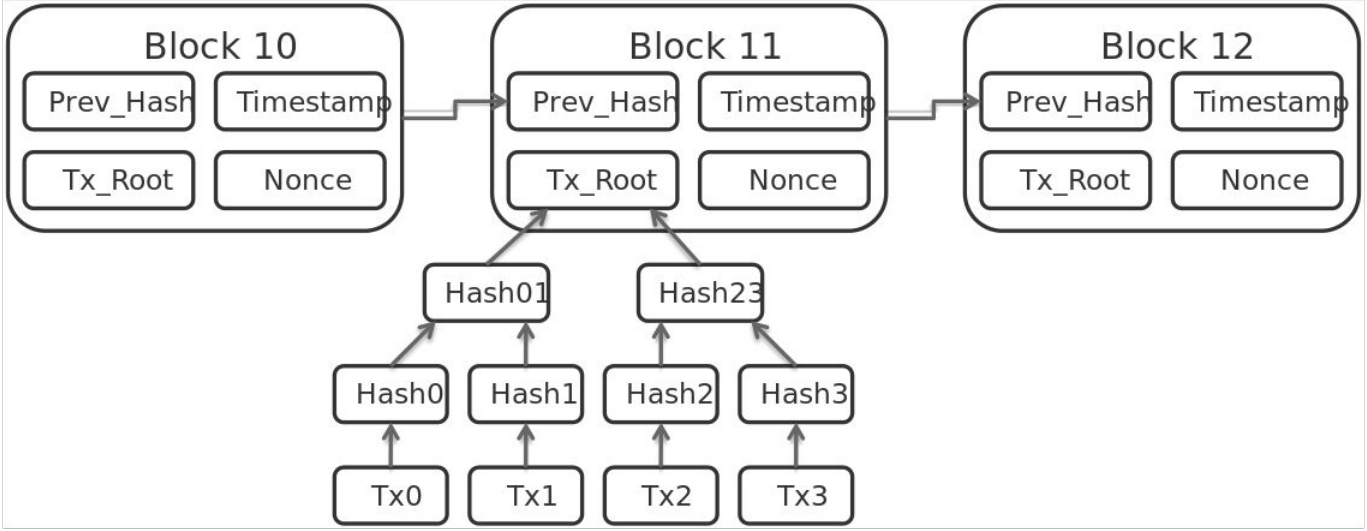
Blockchains are complex
most explanations are nice, but wrong (think Bohr atom)



unchained capital

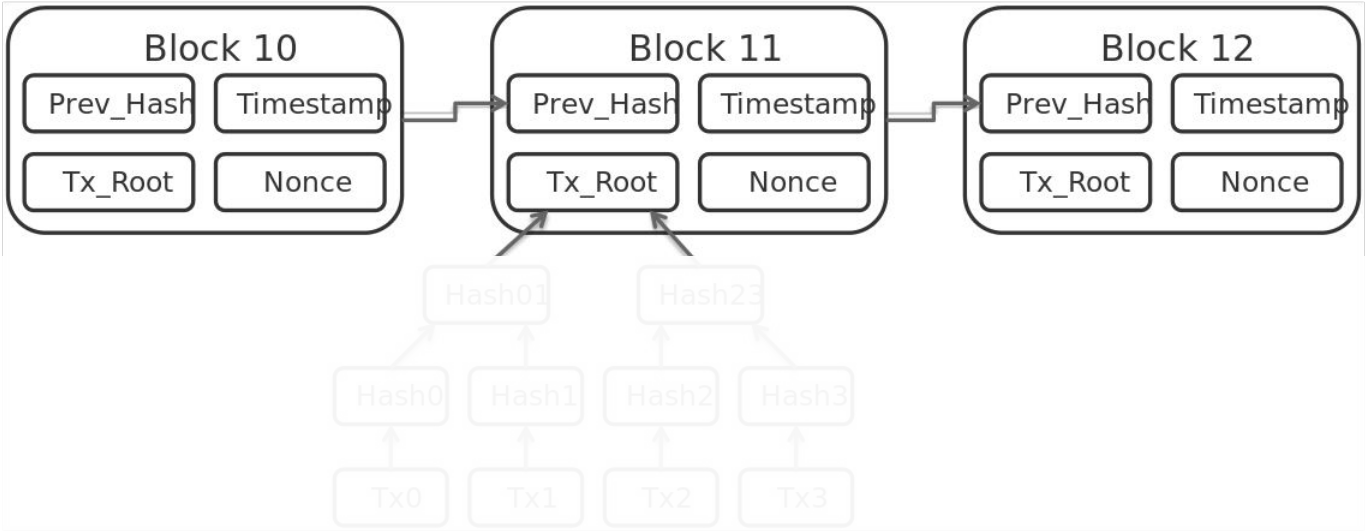
RONOMICAL SOCIETY
cientific understanding of the universe since 1899.

Immutable Data, Fast Look-up/Verify, Hashes for days.



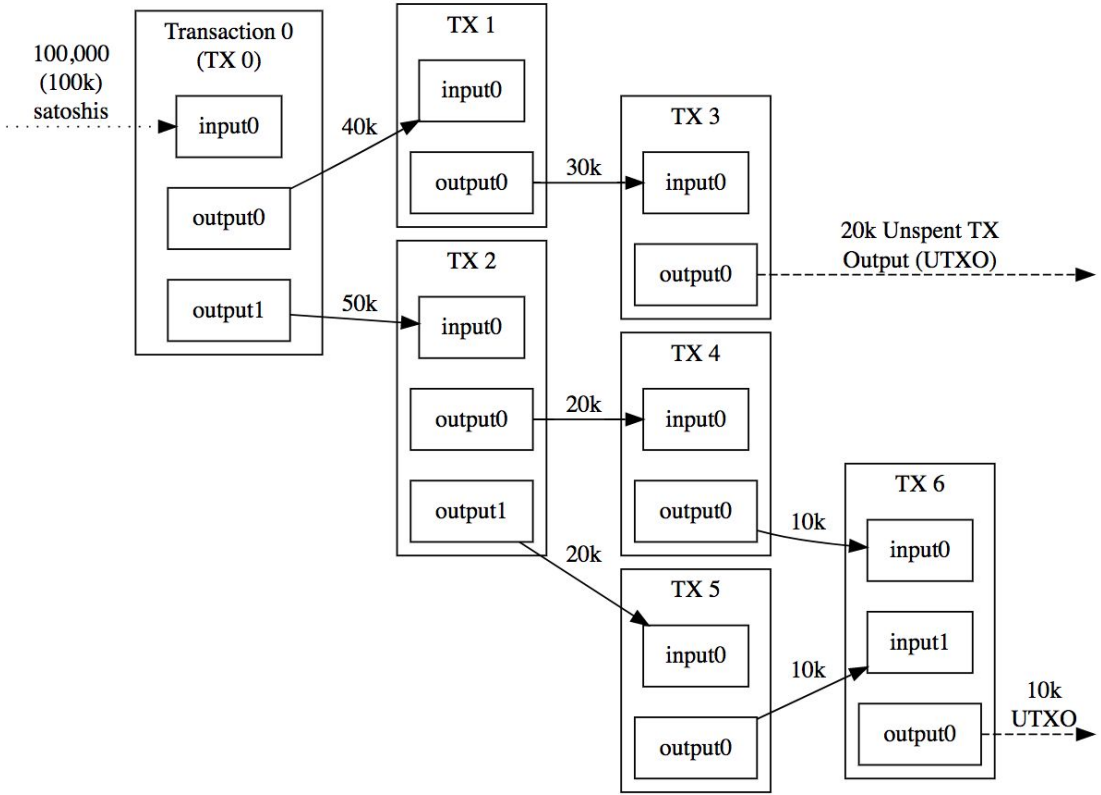
- How the network agrees that a block is valid is the ‘consensus algorithm’.
- Creating a valid block is called ‘mining’.
- For bitcoin, the hash of the block header must be below an adjustable number, this is brute-forced by incrementing through different nonce values.
- Validation uses public-private key cryptography

Immutable Data, Fast Look-up/Verify, Hashes for days.



- How the network agrees that a block is valid is the ‘consensus algorithm’.
- Creating a valid block is called ‘mining’.
- For bitcoin, the hash of the block header must be below an adjustable number, this is brute-forced by incrementing through different nonce values.
- Validation uses public-private key cryptography

Bitcoin transactions reference individual previous transactions, NOT account balances.



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

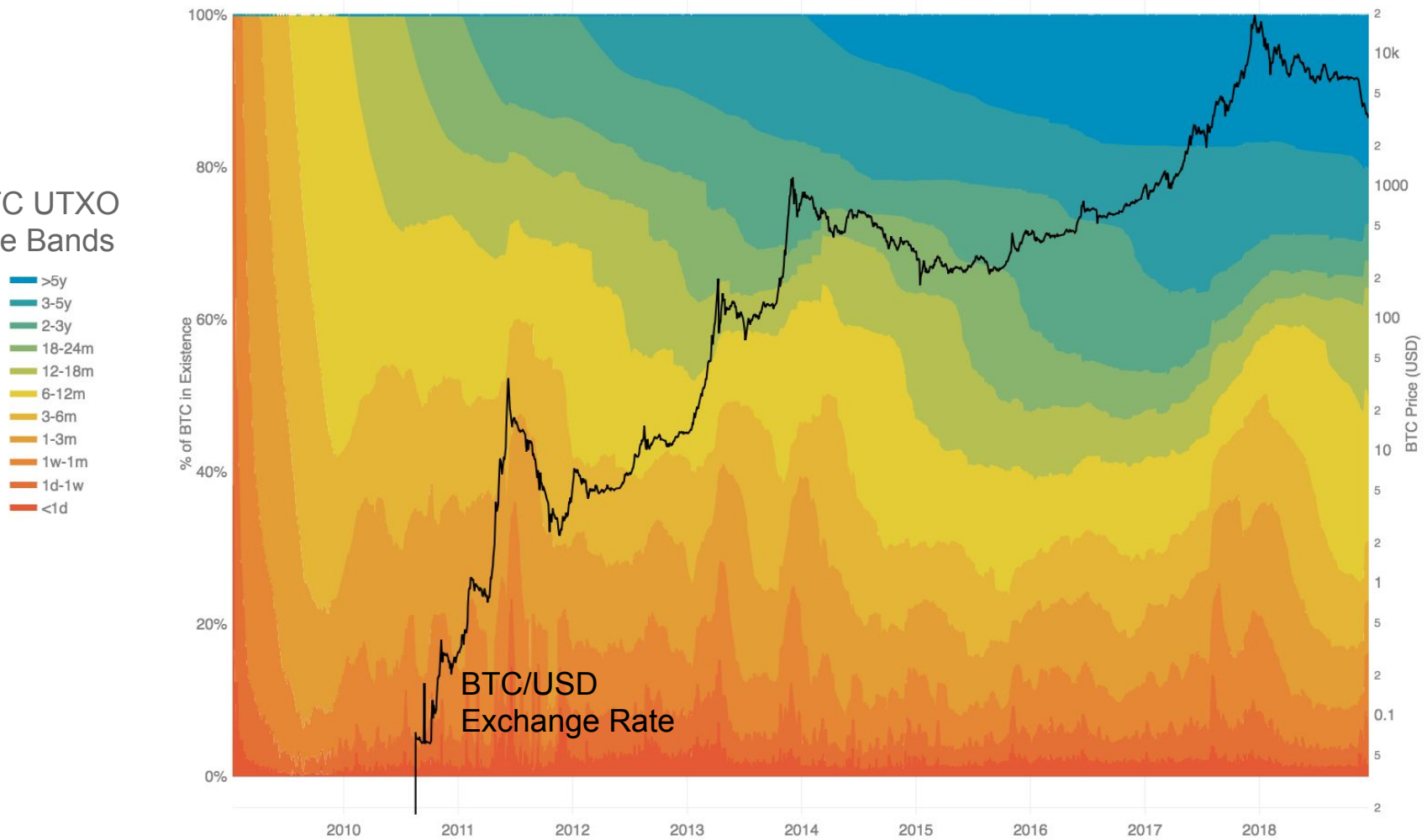
https://bitcoin.org/en/developer-guide#block-chain-overview

The outputs are actually tiny scripts, when you ‘spend’ one you have to provide the correct input such that the script evaluates to ‘true’.

unchained capital

ERICAN ASTRONOMICAL SOCIETY
g and sharing humanity’s scientific understanding of the universe since 1899.

BTC UTXO Age Bands



https://blog.unchained-capital.com/bitcoin-data-science-pt-1-hodl-waves-7f3501d53f63

Blockchains do make new things possible, But it's complicated

- Super secure and accessible
- Protocol & crypto based solutions -
  - Escrows
  - Timelocks
  - Registries
  - Supply Chain & Seed-to-Sale
- Some blockchains use turing-complete languages

But it's not actually magic:

- Access is only as secure as your private key
- External data is difficult to include
- Expensive.
- The network matters (see politics and economics)

I debug, therefore I am.

Why is an Astronomy PhD playing with magic internet money?
Because it's hard problems, and I will not be deterred.

The difficulties:

- Young, poorly funded open source projects
- Off-label (boundary-pushing) use of both hardware and software
- Breaking changes all the time

The 'Rewards':

- Wide range of knowledge necessary
- Always a new problem to solve
- Room for new results / contributions
- Threat modeling requires creativity

unchained capital

AMERICAN ASTRONOMICAL SOCIETY
Enhancing and sharing humanity's scientific understanding of the universe since 1899.

Extra slides

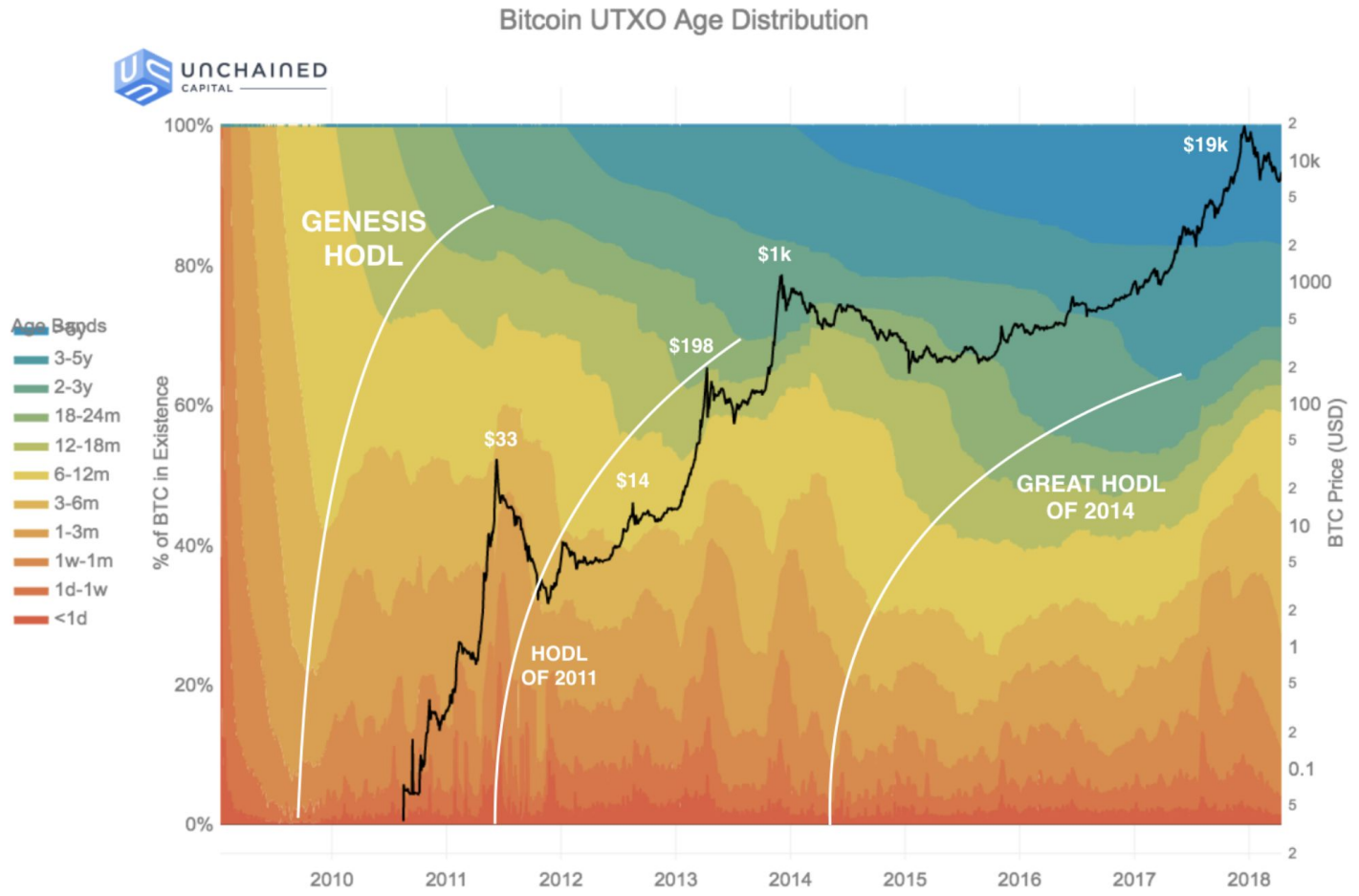
Resources

Huge collection of info - https://lopp.net/bitcoin.html
Satoshi's whitepaper - https://bitcoin.org/bitcoin.pdf (required reading)
Our blog - https://blog.unchained-capital.com/
The O'Reilly Book (it's good!) - Mastering Bitcoin

Bitcoin script example

Standard Transaction to Bitcoin address (pay-to-pubkey-hash)

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
scriptSig: <sig> <pubKey>
```



An annotated image of the UTXO age distribution. Local price peaks are labeled. The solid white lines trace "HODL waves"—a pattern of newly recent Bitcoin aging into each subsequent band, indicating that its new owners are HODLing. Only the three largest HODL waves are traced—many smaller HODL waves are also present.

https://blog.unchained-capital.com/bitcoin-data-science-pt-1-hodl-waves-7f3501d53f63